Amendment to the Claims

1. (currently amended) A process for a simplified access control language that controls
5   access to directory entries in a computer environment, comprising the steps of:

~~providing~~ a system administrator ~~defined~~ creating a read access control list (ACL)
command for a user[[;]], wherein said

~~said system administrator defined~~ read access control list command ~~listing~~ lists a
set of Lightweight Directory Access Protocol (LDAP) user attributes that are ~~selected~~
10   created and controlled by said administrator;

said user applying said read access control list command by listing ~~selecting~~ a
subset from said system administrator defined LDAP user attributes for ~~allowing~~
authorizing ~~user-defined~~ read access to said subset of user attributes to one or more
other users[[;]], and by listing

15   ~~providing a user-defined access control command attribute read list containing~~
user identifications of said one or more other users such that said one or more other
users that are ~~allowed~~ authorized to have read access ~~to~~ said ~~user-defined~~ subset of
said system administrator defined LDAP user attributes; ~~and~~

storing said read access control list command in a directory, said directory
20   containing said user attributes; and

responsive to one or more other users accessing any of said user attributes in
said directory, said read access control list command referring to said ~~user-defined read~~
list of user identifications at runtime thereby allowing said ~~read user identifications~~ one
or more other users read access to said system administrator defined LDAP user
25   attributes[[;]]

~~wherein said read access control command resides in a directory containing said~~
~~LDAP attributes.~~

2. (original) The process of Claim 1, wherein upon a client read access, the directory
30   server selects a specific read access control command according to the attribute being

1

accessed and refers to the read list of the owner of the attribute being accessed to determine if said client has permission to execute said read access.

3. (original) The process of Claim 1, further comprising the steps of:

5   providing a user defined write list containing user identifications that are allowed to write a specified set of attributes;

providing a system administrator defined write access control command;

said write access control command listing the user attributes that said administrator has selected for user.defined write access; and

10   said write access control command referring to said user defined write list thereby allowing said write user identifications write access to said user attributes.

4. (original) The process of Claim 3, wherein upon a client write access, the directory server selects a specific write access control command according to the attribute being

15   accessed and refers to the write list of the owner of the attribute being accessed to determine if said client has permission to execute said write access.

5. (currently amended) A process for a simplified access control language that controls access to directory entries in a computer environment, comprising the steps of:

20   providing for a user a system administrator creating a defined read access control list (ACL) command that lists Lightweight Directory Access Protocol (LDAP) user attributes that said administrator has selected created for user defined read access, said user selecting a subset of user-defined said LDAP user attributes from said list for read access to one or more other users;

25   providing for a user a system administrator creating a defined write access control list (ACL) command that lists Lightweight Directory Access Protocol (LDAP) user attributes that said administrator has selected created for user defined write access, said user selecting a subset of user-defined said LDAP user attributes from said list for write access to one or more other users;

30   providing a plurality of user defined access control list command attribute read lists containing user identifications of said one or more other users that are allowed to

2

read said user defined subset from said LDAP user attributes that said administrator has ~~selected~~ created for user defined read access; ~~and~~

providing a plurality of user defined access control list command attribute write lists containing user identifications of said one or more other users that are allowed to

5 write said user defined subset from said LDAP user attributes that said administrator has ~~selected~~ created for user defined write access; and

~~wherein~~ storing said read access control list command and said write access control list command reside in a directory containing said LDAP user attributes;

wherein ~~when a client~~ responsive to one or more other users requesting read

10 access to one of the LDAP user attributes ~~that said administrator has selected for user defined read access occurs~~, applying said read access control list command and the read list of the owner of the attribute being accessed ~~are used~~ to determine if said ~~client~~ one or more other users has permission to execute said read access; and

wherein ~~when a client~~ responsive to one or more other users requesting write

15 access to one of the LDAP user attributes ~~that said administrator has selected for user defined write access occurs~~, applying said write access control list command and the write list of the owner of the attribute being accessed ~~are used~~ to determine if said ~~client~~ one or more other users has permission to execute said write access.

20 6. (currently amended) A process for a simplified access control language that controls access to directory entries in a computer environment, comprising the steps of:

~~providing~~ a system administrator ~~defined~~ creating a write access control list (ACL) command for a user[[;]], wherein said

~~said system administrator defined~~ write access control list command ~~listing~~ lists a

25 set of Lightweight Directory Access Protocol (LDAP) user attributes that are ~~selected~~ created and controlled by said administrator;

said user applying said write access control list command by listing ~~selecting~~ a subset from said system administrator defined LDAP user attributes for ~~allowing~~ authorizing ~~user-defined~~ write access to said subset of user attributes to one or more

30 other users[[;]], and by listing

3

providing a user defined access control command attribute write list containing user identifications of said one or more other users such that said one or more other users that are allowed authorized to have write access to said user defined subset of said system administrator defined LDAP user attributes; and

5   storing said write access control list command in a directory, said directory containing said user attributes; and

        responsive to one or more other users accessing any of said user attributes in said directory, said write access control list command referring to said user defined write list of user identifications at runtime thereby allowing said write user identifications one

10   or more other users write access to said system administrator defined LDAP user attributes[[;]]

        wherein said write access control command resides in a directory containing said LDAP attributes.

15   7. (original) The process of Claim 6, wherein upon a client write access, the directory server selects a specific write access control command according to the attribute being accessed and refers to the write list of the owner of the attribute being accessed to determine if said client has permission to execute said write access.

20   8. (original) The process of Claim 6, further comprising the steps of:

        providing a user defined read list containing user identifications that are allowed to read a specified set of attributes; and

        providing a system administrator defined read access control command;

        wherein said read access control command lists the user attributes that said

25   administrator has selected for user defined read access; and

wherein said read access control command refers to said user defined read list thereby allowing said read user identifications read access to said user attributes.

    9. (original) The process of Claim 8, wherein upon a client read access, the directory

30   server selects a specific read access control command according to the attribute being

4

accessed and refers to the read list of the owner of the attribute being accessed to determine if said client has permission to execute said read access.

10. (currently amended) An apparatus for a simplified access control language that
5   controls access to directory entries in a computer environment, comprising:
     means for a system administrator ~~defined~~ creating a read access control list (ACL) command for a user[[;]], wherein said
     ~~means for said system administrator defined~~ read access control list command ~~listing~~ lists a set of Lightweight Directory Access Protocol (LDAP) user attributes that
10   are ~~selected~~ created and controlled by said administrator;
     means for said user applying said read access control list command by listing ~~selecting~~ a subset from said system administrator defined LDAP user attributes for ~~allowing~~ authorizing ~~user-defined~~ read access to said subset of user attributes to one or more other users[[;]], and by listing
15   ~~a user defined access control command attribute read list containing~~ user identifications of said one or more other users such that said one or more other users ~~that~~ are ~~allowed~~ authorized to have read access to said ~~user defined~~ subset of said system administrator defined LDAP user attributes; ~~and~~
     means for storing said read access control list command in a directory, said
20   directory containing said user attributes; and
     responsive to one or more other users accessing any of said user attributes in said directory, means for said read access control list command referring to said ~~user defined read~~ list of user identifications at runtime thereby allowing said ~~read user identifications~~ one or more other users read access to said system administrator defined
25   LDAP user attributes[[;]]
     ~~wherein said read access control command resides in a directory containing said LDAP user attributes.~~

11. (original) The apparatus of Claim 10, wherein upon a client read access, the
30   directory server selects a specific read access control command according to the

5

attribute being accessed and refers to the read list of the owner of the attribute being accessed to determine if said client has permission to execute said read access.

12. (original) The apparatus of Claim 10, further comprising:

5   a user defined write list containing user identifications that are allowed to write a specified set of attributes; and

        a system administrator defined write access control command;

        wherein said write access control command lists the user attributes that said administrator has selected for user defined write access; and

10   wherein said write access control command refers to said user defined write list thereby allowing said write user identifications write access to said user attributes.

13. (original) The apparatus of Claim 12, wherein upon a client write access, the directory server selects a specific write access control command according to the

15   attribute being accessed and refers to the write list of the owner of the attribute being accessed to determine if said client has permission to execute said write access.

14. (currently amended) An apparatus for a simplified access control language that controls access to directory entries in a computer environment, comprising:

20   means for a system administrator creating a defined read access control list (ACL) command for a user that lists Lightweight Directory Access Protocol (LDAP) user attributes that said administrator has selected created for user defined read access, said user selecting a subset of user defined said LDAP user attributes from said list for read access to one or more other users;

25   means for a system administrator creating a defined write access control list (ACL) command for a user that lists LDAP user attributes that said administrator has selected created for user defined write access, said user selecting a subset of user defined said LDAP user attributes from said list for write access to one or more other users;

30   a plurality of user defined access control list command attribute read lists containing user identifications of said one or more other users that are allowed to read

6

said user defined subset from said LDAP user attributes that said administrator has ~~selected~~ created for user defined read access; ~~and~~

a plurality of user defined access control list command attribute write lists containing user identifications of said one or more other users that are allowed to write

5   said user defined subset from said LDAP user attributes that said administrator has ~~selected~~ created for user defined write access; and

~~wherein~~ storing said read access control list command and said write access control list command reside in a directory containing said LDAP user attributes;

wherein ~~when a client~~ responsive to one or more other users requesting read

10   access to one of the LDAP user attributes ~~that said administrator has selected for user defined read access occurs~~, applying said read access control list command and the read list of the owner of the attribute being accessed ~~are used~~ to determine if said ~~client~~ one or more other users has permission to execute said read access; and

wherein ~~when a client~~ responsive to one or more other users requesting write

15   access to one of the LDAP user attributes ~~that said administrator has selected for user defined write access occurs~~, applying said write access control list command and the write list of the owner of the attribute being accessed ~~are used~~ to determine if said ~~client~~ one or more other users has permission to execute said write access.

20   15. (currently amended) An apparatus for a simplified access control language that controls access to directory entries in a computer environment, comprising:

means for a system administrator ~~defined~~ creating a write access control list (ACL) command for a user[[;]], wherein said

~~means for said system administrator defined~~ write access control list command

25   ~~listing~~ lists a set of Lightweight Directory Access Protocol (LDAP) user attributes that are ~~selected~~ created and controlled by said administrator;

means for said user applying said write access control list command by listing ~~selecting~~ a subset from said system administrator defined LDAP user attributes for ~~allowing~~ authorizing ~~user-defined~~ write access to said subset of user attributes to one or

30   more other users[[;]], and by listing

7

~~a user defined access control command attribute write list containing~~ user identifications of said one or more other users such that said one or more other users ~~that~~ a re ~~allowed~~ authorized to have w rite a ccess t o s aid ~~user-defined~~ s ubset of s aid system administrator defined LDAP user attributes; ~~and~~

5 means for storing said write access control list command in a directory, said directory containing said user attributes; and

responsive to one or more other users accessing any of said user attributes in said directory, means for said write access control list command referring to said ~~user~~ ~~defined write~~ list of user identifications at runtime thereby allowing said ~~write user~~

10 ~~identifications~~ one or more other users write access to said system administrator defined LDAP user attributes[[;]]

~~wherein said write access control command resides in a directory containing said~~ ~~LDAP user attributes.~~

15 16.(original) The apparatus of Claim 15, wherein upon a client write access, the directory server selects a specific write access control command according to the attribute being accessed and refers to the write list of the owner of the attribute being accessed to determine if said client has permission to execute said write access.

20 17.(original) The apparatus of Claim 15, further comprising:

a user defined read list containing user identifications that are allowed to read a specified set of attributes;

a system administrator defined read access control command;

wherein said read access control command lists the user attributes that said

25 administrator has selected for user defined read access; and

wherein said read access control command refers to said user defined read list thereby allowing said read user identifications read access to said user attributes.

18.(original) The apparatus of Claim 17, wherein upon a client read access, the

30 directory server selects a specific read access control command according to the

8

attribute being accessed and refers to the read list of the owner of the attribute being accessed to determine if said client has permission to execute said read access.

19. (currently amended) A program storage medium readable by a computer, tangibly
5   embodying a program of instructions executable by the computer to perform method steps for a simplified access control language that controls access to directory entries in a computer environment, comprising the steps of:

providing a system administrator defined creating a read access control list (ACL) command for a user[[;]], wherein said
10   said system administrator defined read access control list command listing lists a set of Lightweight Directory Access Protocol (LDAP) user attributes that are selected created and controlled by said administrator;

said user applying said read access control list command by listing selecting a subset from said system administrator defined LDAP user attributes for allowing
15   authorizing user-defined read access to said subset of user attributes to one or more other users[[;]], and by listing

providing a user-defined access control command attribute read list containing user identifications of said one or more other users such that said one or more other users that are allowed authorized to have read access to said user-defined subset of
20   said system administrator defined LDAP user attributes; and

storing said read access control list command in a directory, said directory containing said user attributes; and

responsive to one or more other users accessing any of said user attributes in said directory, said read access control list command referring to said user-defined read
25   list of user identifications at runtime thereby allowing said read user identifications one or more other users read access to said system administrator defined LDAP user attributes[[;]]

wherein said read access control command resides in a directory containing said LDAP attributes.

30

9

20. (original) The method of Claim 19, wherein upon a client read access, the directory server selects a specific read access control command according to the attribute being accessed and refers to the read list of the owner of the attribute being accessed to determine if said client has permission to execute said read access.

5

21. (original) The method of Claim 19, further comprising the steps of:

providing a user defined write list containing user identifications that are allowed to write a specified set of attributes;

providing a system administrator defined write access control command;

10 said write access control command listing the user attributes that said administrator has selected for user defined write access; and

said write access control command referring to said user defined write list thereby allowing said write user identifications write access to said user attributes.

15 22. (original) The method of Claim 21, wherein upon a client write access, the directory server selects a specific write access control command according to the attribute being accessed and refers to the write list of the owner of the attribute being accessed to determine if said client has permission to execute said write access.

20 23. (currently amended) A program storage medium readable by a computer, tangibly embodying a program of instructions executable by the computer to perform method steps for a simplified access control language that controls access to directory entries in a computer environment, comprising the steps of:

providing for a user a system administrator creating a defined read access 25 control list (ACL) command that lists Lightweight Directory Access Protocol (LDAP) user attributes that said administrator has selected created for user defined read access, said user selecting a subset of user-defined said LDAP user attributes from said list for read access to one or more other users;

providing for a user a system administrator creating a defined write access 30 control list (ACL) command that lists Lightweight Directory Access Protocol (LDAP) user attributes that said administrator has selected created for user defined write access,

said user selecting a subset of ~~user defined~~ <u>said</u> LDAP user attributes from said list for write access to <u>one or more</u> other users;

providing a plurality of user defined access control <u>list</u> command attribute read lists containing user identifications <u>of said one or more other users</u> that are allowed to
5 read said user defined subset from said LDAP user attributes that said administrator has ~~selected~~ <u>created</u> for user defined read access; ~~and~~

providing a plurality of user defined access control <u>list</u> command attribute write lists containing user identifications <u>of said one or more other users</u> that are allowed to write said user defined subset from said LDAP user attributes that said administrator
10 has ~~selected~~ <u>created</u> for user defined write access; <u>and</u>

~~wherein~~ <u>storing</u> said read access control <u>list</u> command and said write access control <u>list</u> command reside in a directory containing said LDAP user attributes;

wherein ~~when a client~~ <u>responsive to one or more other users requesting</u> read access to one of the LDAP user attributes ~~that said administrator has selected for user~~
15 ~~defined read access occurs~~, <u>applying</u> said read access control <u>list</u> command and the read list of the owner of the attribute being accessed ~~are used~~ to determine if said ~~client~~ <u>one or more other users</u> has permission to execute said read access; and

wherein ~~when a client~~ <u>responsive to one or more other users requesting</u> write access to one of the LDAP user attributes ~~that said administrator has selected for user~~
20 ~~defined write access occurs~~, <u>applying</u> said write access control <u>list</u> command and the write list of the owner of the attribute being accessed ~~are used~~ to determine if said ~~client~~ <u>one or more other users</u> has permission to execute said write access.

24. (currently amended) A program storage medium readable by a computer, tangibly
25 embodying a program of instructions executable by the computer to perform method steps for a simplified access control language that controls access to directory entries in a computer environment, comprising the steps of:

~~providing~~ a system administrator ~~defined~~ <u>creating a</u> write access control <u>list</u> (ACL) command for a user~~[[;]]<u>, wherein said</u>

11

~~said system administrator defined~~ write access control list command ~~listing~~ lists a set of Lightweight Directory Access Protocol (LDAP) user attributes that are ~~selected~~ created and controlled by said administrator;

said user applying said write access control list command by listing ~~selecting~~ a

5   subset from said system administrator defined LDAP user attributes for ~~allowing~~ authorizing ~~user-defined~~ write access to said subset of user attributes to one or more other users[[;]], and by listing

~~providing a user-defined access control command attribute write list containing~~ user identifications of said one or more other users such that said one or more other

10   users ~~that~~ are ~~allowed~~ authorized to have write access to said ~~user-defined~~ subset of said system administrator defined LDAP user attributes; ~~and~~

storing said write access control list command in a directory, said directory containing said user attributes; and

responsive to one or more other users accessing any of said user attributes in

15   said directory, said write access control list command referring to said ~~user-defined write~~ list of user identifications at runtime thereby allowing said ~~write user identifications~~ one or more other users write access to said system administrator defined LDAP user attributes[[;]]

~~wherein said write access control command resides in a directory containing said~~

20   ~~LDAP attributes.~~

25.(original) The method of Claim 24, wherein upon a client write access, the directory server selects a specific write access control command according to the attribute being accessed and refers to the write list of the owner of the attribute being accessed to

25   determine if said client has permission to execute said write access.

26.(original) The method of Claim 24, further comprising the steps of:

providing a user defined read list containing user identifications that are allowed to read a specified set of attributes; and

30   providing a system administrator defined read access control command;

12

wherein said read access control command lists the user attributes that said administrator has selected for user defined read access; and

 wherein said read access control command refers to said user defined read list thereby allowing said read user identifications read access to said user attributes.

5

27.(original) The method of Claim 26, wherein upon a client read access, the directory server selects a specific read access control command according to the attribute being accessed and refers to the read list of the owner of the attribute being accessed to determine if said client has permission to execute said read access.